Amendments to the Claims

1. (currently amended) A process for modifying an application computer program that is, ~~said application computer program~~ configured ~~in its unmodified form~~ to execute within a first electronic execution environment, said process comprising:

incorporating into said application computer program an execution controller that is configured to execute as a debugger within a second electronic execution environment different from said first electronic execution environment;

identifying boundaries of a subsection of said application computer program; and

modifying said subsection of said application computer program to a form which, when executed within the first electronic execution environment, causes a transfer of execution control to said execution controller, ~~triggers an invocation of a second electronic execution environment different from said computer operating systemfirst execution environment; and~~

~~incorporating with said application computer program control information enabling execution of the application computer program in the second execution environment.~~

2. (original) The process of claim 1 wherein a boundary of said subsection is a flow control instruction.

3. (cancelled) ~~The process of claim 1 wherein the first execution environment is a computer operating system and the second execution environment is a debugging environment.~~

4. (currently amended) The process of claim [[3]] 1 wherein said step of modifying said subsection of said application computer program includes a step of adding an instruction that causes ~~said operating system to~~ a transfer of execution control to said execution controller, ~~said debugging environment~~.

5. (currently amended) The process of claim 1 wherein said step of modifying said

subsection of said application computer program includes a step of encrypting at least a portion of said subsection of said application computer program ~~file~~.

6. (original) The process of claim 5 wherein said step of modifying said subsection of said application computer program further includes a step of relocating at least a portion of said encrypted portion of said subsection to a location distinct from the location of the corresponding unmodified subsection of said application computer program.

7. (currently amended) The process of claim 1 wherein said step of modifying said subsection of said application computer program includes a step of adding functionality for the ~~application computer program~~ execution controller to communicate with a remote process, wherein the remote process does not execute within either the first or second execution environments.

8. (original) The process of claim 7 wherein said remote process is a process that authorizes continued execution of the application computer program.

9. (original) The process of claim 8 wherein said remote process is a cryptographic key management process.

10. (currently amended) The process of claim 7 wherein said ~~application computer program~~execution controller communicates information about execution of said application computer ~~application~~ program.

11. (currently amended) The process of claim 10 wherein said information is information about tampering with said application computer ~~application~~ program.

12. (currently amended) An apparatus for executing an application computer program, comprised of:

a computer with an operating system;

an application computer program having an executable portion in a form that can be executed in a first execution environment under the control of the operating system and a non-executable portion in a non-executable form; and

an execution controller in a form that can be executed as a debugger in a second ~~providing an~~ execution environment under the control of the operating system, said second execution environment distinct from said ~~operating system~~first execution environment, and wherein said execution controller ~~being operable to~~ converts the non-executable portion of the application computer program into a form that can be executed in the first execution environment.

13. (currently amended) The apparatus of claim [[~~13~~]] 12 wherein the non-executable portion of the application computer program includes an encrypted portion.

14. (currently amended) The apparatus of claim 13 wherein the execution controller ~~application computer program includes a portion~~ communicates with a first remote process, and wherein the first remote process does not execute within the first execution environment or the second execution environment. ~~within either the operating system or the execution controller.~~

15. (currently amended) The apparatus of claim 14 wherein the first remote process is a process that authorizes continued execution of the application computer program.

16. (currently amended) The apparatus of claim 15 wherein the first remote process is a cryptographic key management process.

17. (currently amended) The apparatus of claim [[~~14~~]] 12 wherein the execution controller communicates ~~application computer program includes a portion capable of communicating to the remote process~~ information about execution of said application computer ~~application~~ program to a second remote process, wherein the second remote process does not execute within the first

execution environment or the second execution environment.

18. (currently amended) The apparatus of claim 17 wherein the information about execution of said application computer ~~application~~ program is information about tampering with the application computer ~~application~~ program.

19. (currently amended) A process for executing an application [[a]] computer ~~application~~ program, comprising the steps of:

launching an operating system;

launching an application computer program, said application computer program having an executable portion in a form that can be executed in a first execution environment under the control of the operating system and a non-executable portion in a non-executable form;

launching an execution controller, said execution controller in a form that can be executed as a debugger in a second ~~providing an~~ execution environment distinct from the ~~operating system~~first execution environment;

using the execution controller to convert ~~and capable of converting~~ the non-executable portion of the application computer program to an executable form ~~capable of execution~~; and

executing the application computer program within the first execution environment ~~of the execution controller~~.

20. (cancelled) ~~The process of claim 19, wherein the execution controller launches as a debugger.~~

21. (currently amended) The process of claim 19, wherein the non-executable portion of the application computer ~~application~~ program is in encrypted form.

22. (currently amended) The process of claim 19, wherein the ~~application computer program~~execution controller communicates with a first remote process, wherein the first remote

process does not execute under the control of either the ~~operating system~~application computer program or the execution controller.

23. (currently amended) The process of claim 22 wherein the first remote process is part of a cryptographic key management process.

24. (currently amended) The process of claim 19 wherein the ~~application computer program~~execution controller communicates information ~~to the remote process~~ about execution of the application computer program to a second remote process, wherein the second remote process does not execute within the first execution environment or the second execution environment.

25. (original) The process of claim 24 wherein the information is information about tampering with the application computer program.